مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical OS Command Injection Vulnerability in Splunk AI Toolkit

Tracking #:432319155

Date:18-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Splunk has disclosed a critical OS Command Injection vulnerability in the Splunk AI Toolkit. An authenticated user with administrative privileges could exploit the flaw to execute arbitrary operating system commands on the host running Splunk Enterprise, potentially leading to full system compromise.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-20266 – OS Command Injection in btool Configuration Helper**
- **Severity:** Critical | **CVSS:** 9.1
- A vulnerability exists in the btool configuration helper of Splunk AI Toolkit due to an unsafe shell execution pattern. The application constructs OS command strings using dynamic parameters without properly disabling shell interpretation.
- An authenticated user with the admin Splunk role can exploit this flaw to execute arbitrary operating system commands on the host running the Splunk Enterprise instance. Successful exploitation may result in unauthorized command execution and compromise of system confidentiality, integrity, and availability.

Affected Versions

- Splunk AI Toolkit versions prior to 5.7.4

Fixed Versions

- Splunk AI Toolkit 5.7.4 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Splunk.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://advisory.splunk.com/advisories/SVD-2026-0614